**IT Applications, Unit 4**

**Security and ethical considerations, Ch 8, p 294**

Security Equipment

**Security Software**

Describe each of the following software-based security types.

1. Encryption software

Encryption software can be applied to electronic data to ensure that only a authorised user can view in its true form else it will be just displayed as a meaningless jumble of characters. As such this is often used for data transmission to prevent unauthorised access.

* 1. What are the two types of modern encryption methods?
* **Symmetric-Key Encryption** is one of the main methods where both the receiver and sender will have the same shared key installed on their computers. The sender encrypts using their key before sending and then the recipient uses the preinstalled copy of the same key to decipher the message. For this method of encryption to work the intended computers for receiving or sending must be known as they required the key preinstalled.
* **Asymmetric-Key Encryption** is the another of the main methods used being also known as public key encryption. This method uses two keys, a public key given by your computer by sender for recipient to view the file using their private key and a private key to decrypt.

1. Network policies, profiles

Network policies and profiles are also commonly used to protect data accessed via networks. This is a basic step taken by network admin to protect the data held on the networks. Typically this will include a username/password step for authorisation then only supplied files they are permitted by their credentials and hence position in the organisation. Another policy that may be implemented is the constant change of password required at regular intervals as well as ensuring that the password meets certain requirements to ensure that the chance of a successful guess is lower.

1. Firewalls

Firewalls are another type of network protection, used to restrict access by outsiders to a network, as well as to protect confidential information. A firewall is a combination of hardware and software that will only allow for authorised traffic to travel through the allowed ports and from/to allowed programs. This hence is a layer of protection against

1. Antivirus software

Antivirus software is used to prevent computers becoming infected by detecting the presence or patterns and removing/stopping it. They should also detect a virus in a file being downloaded. Once a virus has been detected according to the settings it may either delete or prompt for deletion.

**Security Procedures, p 299**

**Communication:**

1. List the security considerations for communication within an organisation.

* Well documented processes for communicating sensitive information via email, telephone and fax.
* Use of passwords on documents that have sensitive information on it.
* Well documented policy for the use of networked devices within the organisation.

**Storage**

1. **Filenaming conventions**
   1. List the 3 types of information each document should include.

Date stamp (indicates the timeliness)

Variation (ie version)

Name (something meaningful)

* 1. Give an example of a sequential file-naming convention.

Newsletter 2011-11 **03oct**.doc ie 2011-11 part simply shows that for 11th month of 2011 with the 03oct being a sequential file name convention

1. **Location of files**

Location of files is the importance of where you store the file, ensuring that they can easily be located when required.

1. **Backups**
   1. Distinguish between each of the following:
      1. Full backup

A full backup copies all files from a device to a storage medium. As it can take a considerable amount of time it is usually only done once in a time period (week, month ect)

* + 1. Differential backup

A differential backup copies only those files that have been changed since the last full backup. To restore you just restore the full update then the differential one. Benefit is quicker backup, issues may come from the need to restore in two ‘steps’.

* + 1. Incremental backup

Incremental backup is similar to a differential except that it uses more than 2 backup medias and as such only copies files since the last incremental. Quicker backups but slower restore.

1. **Backup timeline**
   1. List good practice in relation to backup timelines.

Ideally a backup should be performed as soon as a file changes to ensure that future financial ramifications won’t occur due to the data loss. Similarly they should follow a backup strategy to ensure that the data is safeguarded whist ensuring minimal disruptions. Data backups should prevent no more than 1 days’ work going missing. Similarly you should have more than one backup media to ensure that if you lose that one, you don’t lose all data, they should also be appropriately labelled. To recover now days must normally occur within minutes.

1. **Location of backup files**
   1. List good practice in the relation to the storage of backup files.

* Ensuring stored in such a way that it is harder/impossible to steal
* Safe from water/fire damage
* Safe from other natural disasters and physical such as shock or magnetic ect.

A fireproof and waterproof safe is generally a good solution for this. They may also benefit from:

* Being stored in a remote location to the business, the further the best as a disaster in one town normally wont effect another while a whole different region or country will rarely be affected at the same time.
* At regular intervals ensuring that the backup works to ensure that in a real situation it wouldn’t be an issue. This may be part of a disaster recovery simulation that should test the overall efficiency and effectiveness of your solution.
  1. What is the grandparent-parent-child system?

The grandparent-parent-child system is a method of backup that a file is backed up incrementally on a daily basis over three days and as such the grandparent backup is the oldest version of file following through to the parent as second oldest and ending with the child that will be the most recent.

Ie a incremental backup is performed each day, differential backup at end of week and a full back up at end of each month.

Note that tis a backup strategy

1. **Archiving and destruction**
   1. Distinguish between archiving and destruction?

Archiving involves copying over to long term storage then deleting from medium while destruction is only the deleting step

* 1. What is a problem for ICT managers?

A key problem for ICT managers is what would be an appropriate storage medium for the archive as it needs to; not deteriorate and still be able to be accessed (X) years down the track by having readers/programs and devices still in working order.

* 1. What is a legacy system?

A legacy system is simply an old system, commonly used for running or accessing old data and programs that may still be needed.

1. **Disposal**
   1. What issues must organisations consider in disposing information?

one of the main issues organisations must consider involves that some data may become required further down the track and as such determining what data to dispose of can be difficult especially when storage space is getting short however this is generally gotten around by generous data strategies. Another issue involves the actual disposal and ensuring that it can’t be recovered.